IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Marc Epstein et al.

Application No.: 09/750,500

Filed: December 28, 2000

For: Architecture For Serving And Managing Independent Access Devices

Confirmation No.: 6952

Group Art Unit: 2457

Examiner: El Chanti, Hussein A.

Attorney Docket No.: 300-2

VIA EFS
Mail Stop Appeal Brief - Patents
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Sir or Madam,

This paper is a reply brief under 37 C.F.R. § 41.41 in response to the Examiner's Answer mailed July 15, 2009 (hereafter referred to as the "Examiner Answer" or the "Answer"). In section (10) of the Answer, the Examiner responds to a selection of the arguments made in Appellants' brief. Appellants now respond to the Answer's arguments as follows in this paper.

I. THE ANSWER MIS-READS ERPELDINGER

Before turning to the specific claim language and specific arguments presented by the Answer, it is worth noting a fundamental error appears to permeate the Answer. Specifically, the Answer cites email services as an example of the first set of services provided by a server to a client (Answer, p. 7) and software distribution from a server to a client as an example of the second set of services provided by a different set of servers. (Answer, p. 9) The Answer then concludes that, with respect to the second set of services (i.e.; software distribution from the server to the client) since "the workstation does not access the distribution server, then Erpeldinger teaches prohibiting secure access to the second set of one or more servers." (Answer at p. 8).

With respect to this second set of services, the Answer has incorrectly translated the fact that software updates go from the server to the client, into a claim limitation that the server securely accesses the client while the client is simultaneously prohibited from securely accessing the server. However, the mere fact that information (e.g.; software updates) goes from the server to the client, or even the fact that the command to perform the client update may be sent from the server to the client, does not mean the server securely accesses the client and that the client is prohibited from securely accessing the server. Instead, it means that after the client first securely accesses the servers via an authenticated password/login, the server may then provide software updates, just like the server may provide the first set of services, email services, or any other services.

With respect to the security required for a client to access any server, and regardless of whether the server provides software updates, email, or any other service, Erpeldinger says nothing about treating servers that provide a first set of services to clients differently from other servers that provide a second set of services to clients – because access to all servers is the same. While Erpeldinger says nothing about secure access at all, assuming email systems inherently require authentication as the Answer argues at p. 7 (no such disclosure exists in Erpeldinger), there is simply nothing in Erpeldinger to even remotely suggest that security of the access by the client to the servers that provide email services is any different from the manner in which security is implemented when a client accesses servers for software updates, or for any other service. [1]

Erpeldinger does discuss clients accessing servers in several places, but all of those places say nothing about implementing one-way trusts in a first direction for a first set of services on a first set of servers and another set of one-way trusts in a second direction –opposite the first direction- for a second set of services on a second set of servers. Moreover, other portions of Erpeldinger strongly imply that such trusts do not exist. First, at col. 1, lines 25-34:

[1] In fact, the email server, which the Examiner uses as an example of the secure access in the opposite direction that of the software updates, also sends information (i.e.; emails) to the client computer, and can also initiate the process to transmit an email to a client, just as another server can send software updates to that client.

> A server is a computer which provides services to several users at the same time. Such services can be data services (price lists, employee records, . . .) application services (e.g. ordering, payroll, . . .) or other services such as printing, electronic mail or software distribution. Depending on the implementation, a server may provide several services or types of services. Of course, several users can connect to one server and use the same service and a user may connect to several servers to use different services.

The above implies that plural servers provide plural services to users, but there is not the slightest suggestion that the security used to access to any server providing one type of service should be treated differently from the security used to access any other service - regardless of which way information flows.

At col. 2, lines 56- 60, Erpeldinger notes that the network "includes a plurality of workstations, 12, 14, 16, 18, which are connected thereto and which share the services provided by several servers 20, 22, 24." Nothing in this section indicates that the security arrangement (such as restrictions on granting secure access to one device by any other device) varies as a function of the type of service being provided by each of servers 20, 22, or 24. The cited text tends to indicate whatever security arrangement exists (Erpeldinger is essentially silent regarding its access/security arrangement) is uniform among the various servers.

Applicants here do not deny that the software distribution server of Erpeldinger can initiate a software update operation by sending a command to the client computer. However, the mere fact that a server can send a command initiating an operation on the client computer does not imply that the server can securely access the client, and that the client cannot securely access that same server, and that the same client can securely access other servers providing other services, and that the other servers providing those other services cannot securely access that same client. Given that

most servers provide plural services, it is nearly impossible for such a situation to exist in Erpeldinger.

Instead, all Erpeldinger teaches about software updates is that once a client accesses the update server in whatever same manner it accesses the other servers, the software update server can optionally send a command to the client to initiate an operation on the client. Absent the same secure access to the software distribution server that is used to access any other server, the client in Erpeldinger cannot get any software updates – whether initiated by the client or the server.

Not only is the Answer's position unsupported in Erpeldinger, but in fact, Erpeldinger specifically refutes the Answer. Specifically, claim 12 of Erpeldinger recites, in relevant part (emphasis added):

> A method of changing a current operating system to a new operating system in a workstation…using a data transmission network **to interconnect to a server** being a software distribution server…executing a software distribution application **in the workstation;** establishing a network session **with the software distribution server**...

Erpeldinger thus strongly implies, if not affirmatively states, that it permits the client to access the server using the software distribution application, in order to establish the network session between the client workstation and the software distribution server. Thus, the statement that "the workstation does not access the distribution server," (Answer, p. 9) is simply incorrect.

Further, Erpeldinger notes that the update "operations can be started from the software distribution server in the preferred embodiment, although other modes of operation are also possible [i.e.; the update operations can start from the client, instead of the server]" (col. 3, lines

15-20). Again, the Answer ignores Erpeldinger when it states that Erpeldinger prohibits access to the software distribution server by the client.

Hence, even if the fact that a server can initiate a software update could be equated to providing secure access from the server to the client – an erroneous proposition in view of what Erpeldinger teaches - the Answer's position would still be incorrect. No place does Erpeldinger teach prohibiting secure access to the same server by that client. Instead, Erpeldinger discloses embodiments where the client does in fact access that same server.

In short, and as explained best at pp. 5-8 of the present specification, the present invention separates the services provided into those where the user login and authentication information of the first set of servers is honored by the client computers served, and those where the user login and authentication information of the client computer is honored by the second set of servers serving the client computers. Trusted connections in the opposite direction are not permitted.

To anticipate the present claims, a system like Erpeldinger would have to be modified to teach a server being provided with a right of secure access to a client, such as by logging on to a client with user ID and password so the client can be sure of the authenticity of the server, while the same client is provided with a right of secure access to another server, such as by having the client log on to the other server by itself providing a different user ID and password so the server can be sure of the authenticity of the client, and each server never providing services that require the user ID and password in the opposite direction, and never permitting access when the authentication was in the wrong direction. In other words, the trusts must be backwards with respect to each other.

As discussed more fully below with respect to each independent claim, Erpeldinger does not disclose two sets of servers that provide services to a client, with the back to back one way trusts of the present invention. Otherwise stated, to meet the limitations of Applicants' claims, the Answer has effectively modified the Erpeldinger reference with teachings drawn from Applicants' own disclosure to allege that Erpeldinger teaches separating the services into two distinct sets, then providing the two sets of services on two respective sets of servers, and still further, implementing differently directed one-way trust arrangements between (a) the first set of servers and the clients and (b) the second of servers and the clients. In fact, Erpeldinger is silent with respect to the above-mentioned features of separation of services into separate/distinct sets; implementation of the separate sets of services on respective separate sets of servers; and implementation of different security arrangements for the two separate servers. Applicants elaborate below with more specific reference to the features of each of the independent claims.

II. The Independent Claims are Patentable

The M.P.E.P. recites that "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); and M.P.E.P. § 2131. With respect to the Examiner's reliance upon inherency, the M.P.E.P. recites "the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993)."

The M.P.E.P. further recites "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the

allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original). Inherency may not be established by mere possibilities or speculation.

Turning to the specific claim language in issue, claim 40 states as follows (emphasis added):

> 40. A method for a service provider to provide services to a plurality of client computers, the method comprising:
>
> providing a first set of services on a first set of one or more servers of the service provider to the plurality of client computers **by providing secure access to the first set of one or more servers by the plurality of client computers, but prohibiting secure access to the plurality of client computers by the first set of one or more servers**; and
>
> providing a second set of services on a second set of one or more servers of the service provider to the plurality of client computers **by providing secure access to the plurality of client computers by the second set of one or more servers, but prohibiting secure access to the second set of one or more servers by the plurality of client computers**.

The Answer does not cite anywhere in Erpeldinger where the bolded limitations are taught. Instead, the Answer appears to speculate that 1) the software distribution server is Erpeldinger could possibly be arranged to do nothing else, and therefore, be separate from the servers that provide other services, such as email; 2) that there is an email server in Erpeldinger; 3) that the email server provides secure access by the client to the server through a login; 4) that the same email server is prohibited from securely accessing the client; 5) that the software distribution server provides secure access by the server to the client by securely logging into the client, and hence, is set up to be accessed differently from the email server, 6) that the same software distribution server prohibits secure access to it; and 7) that neither the email server nor the

software distribution server is in a two-way trust relationship with any client, even though such two-way trusts are extremely widely practiced in the computer network arts.

Inherency may not be based upon speculation about missing claim limitations. *In re Rijckaert, Supra.* Here, to the extent Erpeldinger discusses access to servers by client computers, all the servers are treated the same way, and may be accessed by the clients, whether or not that access is secure, and whether or not the servers can also access the client computers in the other direction securely. Erpeldinger simply does not disclose, either expressly or inherently, any of the four claim limitations that are bolded in the above-quoted claim text.

Identical reasoning is applicable to claim 51.

With respect to the remaining independent claims 62, 66, and 67, these claims require separation of services into server groups, wherein the servers in one group provide services to a client with a one way trust in one direction, and the second group of servers provide services to the same client using a one way trust in the opposite direction. As the specification explains (p. 5), a trust is "a link between domains that enables pass-through authentication, in which a trusting domain honors the logon authentication of a trusted domain."

Thus, claims 62, 66, and 67 define a system in which the client receives services from a first and second set of servers. For the first set of servers, there is a one-way trust connection from the servers to the client computers, which may be implemented by having the servers honor the logon and authentication information of the client computers. For the second set of servers, there is a one-way trust connection from the client computers to the second set of servers, which may be implemented by having the client computers honor the logon and authentication information of the servers. Thus, the two trust connections extend in opposite directions.

These claims are shown below:

62. A method for a service provider to provide services to a plurality of client computers, the method comprising:

separating the services provided by the service provider into a first group of services provided by a first group of one or more servers of the service provider, and a second group of services provided by a second group of one or more servers of the service provider;

providing the first set of services from the first set of servers through a one-way trust connection from the first set of servers to the client computers; and

providing the second set of services from the second set of servers to the client computers through a one-way trust connection from the client computers to the second set of servers.

66. A method for providing services from a service provider to a plurality of client computers, the method comprising:

enabling a first set of services on a first set of servers of the service provider through a one-way trust connection from the first set of servers to the plurality of client computers;

enabling a second set of services on a second set of servers of the service provider to the plurality of client computers through a one-way trust connection from the client computers to the second set of servers; and

providing the first and second sets of services.

67. A system for providing services to a plurality of client computers, the system comprising:

a first set of servers for providing a first set of services to the plurality of client computers through a one-way trust relationship from the first set of servers to the plurality of client computers; and

a second set of servers for providing a second set of services to the plurality of client computers through a one-way trust relationship from the plurality of client computers to the second set of servers.

Erpeldinger does not disclose the claimed "one way" trust, defined at pp. 7-8 of the present specification and recited in each of claims 62, 66, and 67. Specifically, to anticipate the subject matter of claims 62, 66, and 67, the services provided by the different servers would have to be carefully separated among the servers. Next, to get services from the first set of servers, the client

computer would have to logon and provide a user name and password. Servers in this set could not log on to the client computers by supplying a user name and password.

To get other services from a second set of servers, the servers would have to logon to the client to provide services. For servers that provide these second services, the clients could not log on to the servers by providing a user name and password. With respect to which servers provide which services, the system would have to be set up so that servers which provide services requiring the trust in one direction do not also provide services that require the trust in the other direction, and vice versa.

Yet, nothing in Erpeldinger discloses a client authenticating and trusting a server, or a client treating any server any differently from any other server, or even which servers provide which services, and which direction the trust should be in for any service provided by any server. In short, a "one way trust" recited in claims 62, 66, and 67 and defined at least at page 5, and pp. 7-8 of the present specification does not necessarily flow from the use of the server to provide software distribution to workstation computers as in Erpeldinger. Claims 62, 66, and 67 are not anticipated by Erpeldinger, and are not inherently disclosed by Erpeldinger.

III. CONCLUSION

In view of the foregoing, it is submitted that the Final rejection of the pending claims is improper and should not be sustained. Therefore a reversal of the final rejection of September 23, 2008 is respectfully requested. It is believed that no fees are due. However, the Commissioner is hereby authorized to charge any further fees believed due from, or credit any overpayment to, our Deposit Account No. 50-4711.

Dated: September 15, 2009

Respectfully submitted,

By: /Leslie S. Garmaise/
Leslie S. Garmaise
Registration No.: 47,587

and

/Jeffrey I. Kaplan/
Jeffrey I. Kaplan
Registration No.: 34,356

KAPLAN GILMAN & PERGAMENT LLP
1480 Route 9 North, Suite 204
Woodbridge, New Jersey 07095
732-636-4500
Attorneys for Applicant